

Listing of Claims:

Claims 1-30 (canceled)

Claim 31. (new) A method comprising:

selecting for encryption at least every Nth data packet between consecutive data packets having a sequence header code of a data packet sequence to provide a plurality of selected packets and a plurality of unselected data packets;

encrypting the selected data packets; and

initiating the transmission of the encrypted data packets and unselected data packets as an output data packet sequence in a transmission medium.

Claim 32. (new) The method of claim 31, further comprising selecting the value of N based, at least in part, on available processing resources for encryption at a data source and/or available processing resources for decryption at a data destination.

Claim 33. (new) The method of claim 32, wherein the data source is an SSL server and wherein the data destination is an SSL client.

Claim 34. (new) The method of claim 31, wherein the data packet sequence comprises an MPEG data packet sequence.

Claim 35. (new) An apparatus comprising:

logic for selecting for encryption at least every Nth data packet between consecutive data packets having a sequence header code of a data packet sequence to provide a plurality of selected packets and a plurality of unselected data packets;

logic for encrypting the selected data packets; and

logic for initiating the transmission of the encrypted data packets and unselected data packets as an output data packet sequence in a transmission medium.

Claim 36. (new) The apparatus of claim 35, further comprising logic for selecting the value of N based, at least in part, on available processing resources for encryption at a data source and/or available processing resources for decryption at a data destination.

Claim 37. (new) The apparatus of claim 36, wherein the data source is an SSL server and wherein the data destination is an SSL client.

Claim 38. (new) The apparatus of claim 35, wherein the data packet sequence comprises an MPEG data packet sequence.

Claim 39. (new) A system of transmitting a data stream in a transmission medium, the system comprising:

a data transmission source comprising:

logic to select for encryption at least every Nth data packet between consecutive data packets having a sequence header code of a data packet sequence to provide a plurality of selected packets and a plurality of unselected data packets;

logic to encrypt the selected data packets; and

logic to initiate the transmission of the encrypted data packets with the unselected data packets as an output data packet sequence in the transmission medium; and

a data destination adapted to receive the transmitted output data packet sequence.

Claim 40. (new) The system of claim 39, further comprising logic to select the value of N based, at least in part, on available processing resources for encryption at the data transmission source and/or available processing resources for decryption at the data destination.

Claim 41. (new) The system of claim 40, wherein the data transmission source is an SSL server and wherein the data destination is an SSL client.

Claim 42. (new) The system of claim 39, wherein the data packet sequence comprises an MPEG data packet sequence.

Claim 43. (new) An article comprising a machine-accessible medium having stored thereon instructions that, when executed by a machine, cause the machine to:

select for encryption at least every Nth data packet between consecutive data packets having a sequence header code of a data packet sequence to provide a plurality of selected packets and a plurality of unselected data packets;

encrypt the selected data packets; and

initiate the transmission of the encrypted data packets with the unselected data packets as an output data packet sequence in a transmission medium.

Claim 44. (new) The article of claim 43, the machine-accessible medium having stored thereon further instructions that, when executed by a machine, cause the machine to:

select the value of N based, at least in part, on available processing resources for encryption at a data source and/or available processing resources for decryption at a data destination.

Claim 45. (new) The article of claim 44, wherein the data source is an SSL server and wherein the data destination is an SSL client.

Claim 46. (new) The article of claim 43, wherein the data packet sequence comprises an MPEG data packet sequence.